خوارزمية التشفير DES

إعداد عبد الرحمن غسان زعرور

باشراف المهندس طرفة المحمد

بسم الله الرحمن الرحيم وأفضل الصلاة وأتم التسليم على سيدنا محمد وعلى آله وصحبه وسلم

لمحة عن الكاتب:

عبد الرحمن غسان زعرور طالب في معهد تقنيات الحاسوب في المعهد المتوسط لتقنيات الحاسوب في محافظة حماه من سورية درست في ثانوية دلال المغربي لتقنيات الحاسوب في محافظة حمص

اختصاص شبكات الحاسوب أقوم الآن بإتباع دورة CCNA وأريد التقدم لامتحان في CCNA

الإهداء:

أهدي هذا الكتيب المتواضع إلى والدي ووالدتي الذين طالما سهرا وتعبا معي جداً حتى وصلت إلى ما أنا عليه الآن وإلى جميع المدرسين الذين قاموا بتدريسي في جميع المراحل الدراسية وبالخصوص

الأستاذ م. محمود محمد أيوب

الأستاذ عبيدة سمير الطحلة

الأستاذ غسان شربك

الآنسة م.شيماء سلطان

الأستاذ م. طرفة المحمد

الأستاذ م. عدنان الطيار

وإلى ابن العم الغالي الذي طالما احترق لينير بصيرتي بالعلم والمعرفة

المهندس عبيدة محمد خالد زعرور

وإلى كل مسلم في العالم ولكل طالب للعلم

خوارزمية التشفير DES

يخطر في بال معظم الناس عند الحديث عن أمن الشبكات الإنترنت جدران النار وعلى الرغم أن برامج جدران النار لا تعتبر علاجا لجميع مشاكل أمن المعلومات على شبكة الإنترنت إلا أنها ضرورية في أمن الإنترنت . إلا أنه تم استخدام ما يعرف بالتشفير .

أولا:

تعريف التشفير : هو عملية استخدام صيغة ما تدعى خوارزمية التشفير لترجمة النص العادي إلى شفرة غير مفهومة ثم تحويله من جديد إلى نص عادي ويعتمد نص التشفير بشكل أساسي على استخدام قيمة عددية تدعى المفتاح Key وتعد جزءً من خوارزمية التشفير وتعد مسؤولة عن بدء عملية التشفير .

ويتوفر الكثير من خوارزميات التشفير إلا أن أكثرها انتشارا هي خوارزمية DES التي تعتمد على استخدام مفتاح التناظر Symmetric Key أو مفتاح سري Secret Key والتي سيكون شرحنا عنها بشكل إنشاء الله .

"Data Encryption Standard "DES

تم اختياره في عام ١٩٧٧م من قِبل المعهد الدولي للمعايير التكنولوجية أو

National Institute Standard(NIST)على أنه معيار للتشفير دوليا و يتم التطوير على أساسه في أنواع التشفير التي هي من فأته مثل التشفير بالمفتاح المتناظر

ولقد كان لشركة IBM باعا في وضع بذرة هذا التشفير

التشفير بالمفتاح المتناظر

في هذه الطريقة يستخدم نفس المفتاح للعمليتين يوفر التشفير بالمفتاح المتناظر الفائدتين التاليتين :

١- الفعالية : حيث أن المستخدمين لا يعانوا من تأخير طويل نتيجة عمليتا التشفير وفك التشفير.
٢- إثبات الهوية : يمنح التشفير بالمفتاح العام درجة مقبولة من إثبات هوية طرفي الاتصال حيث أنه لا يمكن فك تشفير المعلومات باستخدام مفتاح آخر غير الذي استخدم في التشفير، ويستطيع الطرفان التحقق من هوية الطرف الآخر طوال فترة بقاء المفتاح التناظر غير معروف لطرف ثالث وطالما أن المعلومات المستقبلة لها معنى وضمن المعقول.

الخوارزمية المتناظرة DES

صممت الخوارزمية من قبل NIST وذلك لغرض حماية المعلومات غير المصنفة داخل الولايات المتحدة.

تم اعتماد طول المفتاح ليكون ٦٤ بت ولكن يستعمل منها فقط ٥٦ بت فقط بشكل فعال وتستعمل الباقية كخانات تدقيق للأخطاء، وبما أن الخوارزمية متناظرة يستعمل نفس المفتاح للتشفير وفك التشفير وبالرغم من إمكانية اختراق خوارزمية DES فإنها مازالت تستخدم بشكل كبير ولكن تم استبدالها في الآونة الأخيرة بخوارزمية Treble DES حيث يتم تطبيق خوارزمية DES ثلاث مرات بمفاتيح مختلفة.

ويوجد عدة إصدارات لخوارزمية DES وهي

SDES

STANDAR (DES)

DOUBL DES

TRUBLE DES

SDES(simple Data Encryption Standard):

سوف نتوسع في شرح هذا النوع من التشفير في خوارزمية DES لأنه أبسط نوع من هذه الأنواع وسوف يكون تعاملنا في شرح مثال عن الخوارزمية باستخدام النظام الثنائي

ويجب أن نفهم بعض المصطلحات أو التعاريف لنبدأ بعملية التشفير

١- Initial Permutation (IP) : وهي تبديل المبدئي للبيانات المراد تشفيرها ووظيفتها إدخال ٨بت نقوم بتغير أماكنها بشكل غير منظم بناءً على أرقام تم تحديدها بطلبنا وتكون من رقم ١ إلى ٨ ولكن هذه الأرقام غير مرتبة

١: لدينا الدخل يتكون من مفتاح k=(1…….10)

وينتج لدينا مفتاحين للتشفير هما K1&K2

2: لدينا نص يتكون من ٨بتات

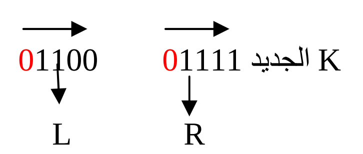
المرحلة الأولى:

نحصل على المفتاحين K1&K2 من المفتاح K

K= (1011011010) (مرقمة 1 2 3 4 5 6 7 8 9 10)

PK(K5,K7,K1,K8,K10,K2,K3,K9,K4,K6)

الـ PK يختاره المشفر ومعنى ذلك أن المستخدم هو من يختاره



ب- ندير كل جزء يميني ويساري دورة واحدة (دورة يسارية واحدة) بمقدار خانة واحدة

L (1 2 3 4 5)	R (6 7 8 9 10)
(11000	11110)

ج- لدينا الثابت(P8) التالي لإخراج K1 من K



6	3	7	4	8	5	10	9
1	0	1	0	1	0	0	1

د- من أخر KEY تم التعديل عليه ندير الجزء اليميني واليساري بمقدار خانتين

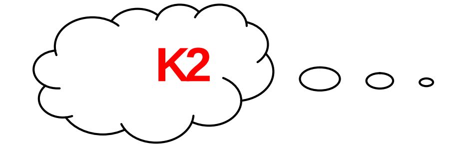
L (1 2 3 4 5)	R (6 7 8 9 10)
(11000	11110)

وبعد التدوير

L (1 2 3 4 5)	R (6 7 8 9 10)
(000 11	11011)

نحصل على K الجديد

نطبق ثابت الاختيار (P8) على K الجديد



6	3	7	4	8	5	10	9
1	0	1	1	0	1	1	1

نكون قد حصلنا على K1 و K2 من K

المرحلة الثانية:التشفير باستخدام k1وk2 (المكونين من ٨ خانات)

-النص مكون من ٨ خانات

PLAIN TEXT= 11001001 (1 2 3 4 5 6 7 8)

١- نبدل المواقع حسب الثابت IP (الثابت) كما يلي :

	L				R			
IP=	2	6	3	1	4	8	5	7
(PLAIN TEXT) P=	1	0	0	1	0	1	1	0

٢- $F_k(L,R)=(L \oplus F(R,SK),R)$

نأخذ الجزء اليميني من المفتاح K1

R= 0 1 1 0

S0=N4(XOR)K1,N1(XOR)K2,N2(XOR)K3,N3(XOR)K4 خانات الجزء اليميني

S1=N2(XOR)K5,N3(XOR)K6,N4(XOR)K7,N1(XOR)K8

S0:0(XOR)1,0(XOR)0,1(XOR)1,1(XOR)0

S0: 1 , 0 , 0 , 1

S1: 1(XOR)1,1(XOR)0,0(XOR)0,0(XOR)1

S1: 0 , 1 , 0 , 1

نأخذ الخانة الأولى والأخيرة من $S0(11)_2$ ⟵ $(3)_{10}$ وهي رقم السطر في s0́

نأخذ الخانة الثانية والثالثة من S0 $(٠٠)_٢$ ⟵ (٠) وهو رقم العمود في s04+6́

وبنفس الطريقة نحصل على خانتين من S1

رقم السطر $(01)_2$ ⟵ $(1)_{10}$

$(1)_{10}$ ⟵ $(01)_2$ حصلنا على خانتين من S1

رقم العمود $(10)_2$ ⟵ $(2)_{10}$

S-Box:هي عملية تبديل لكنها مختلفة تماما عن سابقاتها لكنها ستتسبب في تقليص عدد البتات بقيمة ٢ بت

وتستخدم التبديل في المصفوفات لإيجاد قيمتها ويتم استخراج القيمة من تقاطع الصف مع العمود ومن ثم تحويله إلى ثنائي (يستخرج الناتج بشكل عشري ويتم تحويله إلى ثنائي)

S0́	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	٣
3	3	١	٣	2

Ś 1	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

S0	S1
11	01

نجري تبديل عليها على أساس الثابت التالي

P4=2 4 3 1

1 1 0 1

وهو خرج f(r,sk)

F(R,SK)=P4: 1101

أعوض في FK فيصبح لدينا

FK(L.R)=1001 (XOR) 1101,0110)=(0100,0110)= 0100 0110

المرحلة الثالثة :

نجري تبديل بين الجزئيين اليميني واليساري على FK

0110 0100

L R

المرحلة الرابعة :

نجري التابع FK(L,R) على الناتج الجديد باستخدام K2 فنحصل على ٨خانات (نفس العملية في المرحلة الثانية)

المرحلة الخامسة :

اجري التبديل لأحصل على P-1 وهو النص المشفر حسب القانون التعالي

P-1= 4 1 3 5 7 2 8 6

وبذلك نكون قد حصلنا على النص المشفر

مع تحيات عبد الرحمن غسان زعرور

سورية – حمص – موبايل ٠٩٤٧/٦١٥٧٤١

E-mail: theprince-za08@hotmail.com

إن ما كتبته ما هو إلا من فضل الله وما نسيت أن أذكره فما هو إلا من ذنوبي وخطاياي

الرجاء من جميع من يقرأ الكتاب أن يرسل لي تقييم على الإيميل التالي:

Aleman.com@windowslive.com